University Undergraduate Lectures in Mathematics
A First Year Course

GROUP THEORY

The Mathematics of Symmetry

G R O U P   T H E O R Y   I

Lecture 1

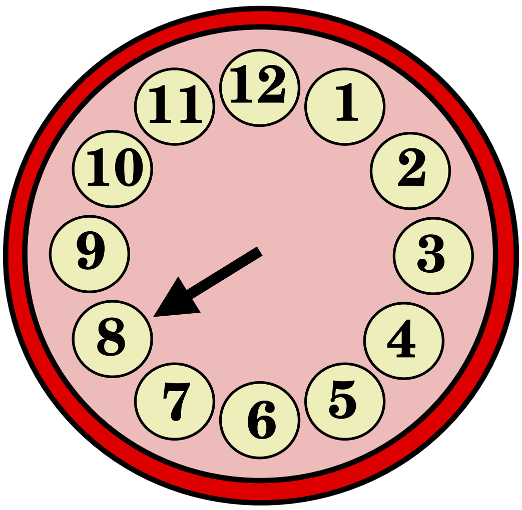
University Undergraduate Lectures in Mathematics
A First Year Course
Group Theory I

1.1 Introduction

Welcome to the world of Group Theory.
In this series of lectures, the underlying theme is “symmetry”, a familiar idea from schoolwork where, for example, reflections and rotations of simple shapes are studied. However, other mathematical entities can have “symmetry”.
For example, a carefully chosen set of numbers or functions.
To tease out the underlying symmetry of such seemingly different entities, mathematics uses a powerful tool; Group Theory.
These lectures are suitable for new undergraduate students for they assume only competence with GCSE mathematics. A second set of Lectures, Group Theory II, is for study towards the end of a first year at University.

1.2 Clock Arithmetic

Imagine an analogue clock that works fine, but has lost its minute hand.
It reads 8 O'clock.
Exactly five hours later, it will read 1 O'clock.



It would be confusing to write the following statement as a description of the situation just considered;

$$8 + 5 = 1$$

And yet, for our clock, this is true !

The way a mathematician would write the calculation is like so;

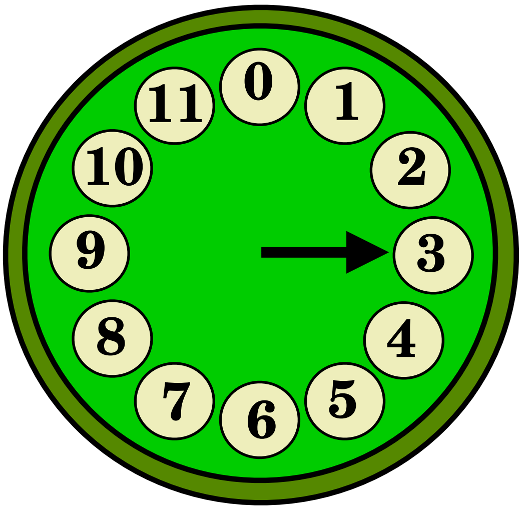
$$8 + 5 \equiv 1 \pmod{12}$$

and they would say, “Eight plus five is congruent to one, modulo twelve”
The word “modulo” is often simply said “mod”.

1.3 A Mathematician Quirk

In measuring time, a traditional clock face features the integers 1 to 12 inclusive. However, in the world of modulo 12 arithmetic, mathematicians' prefer to work with the following set of integers;

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$



Have you spotted the mathematicians' quirk ?

Rather than write,

$$3 + 9 \equiv 12 \pmod{12}$$

a mathematician would write,

$$3 + 9 \equiv 0 \pmod{12}$$

The set {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11} is termed the least residues modulo 12

1.4 Exercise

Solve the following congruence equations modulo 12

Answers should be given as elements from the set of least residues modulo 12

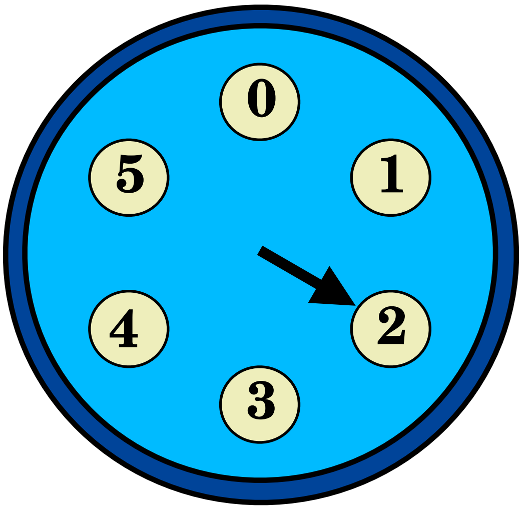
(i) $6 + 9 \equiv x \pmod{12}$ **(ii)** $10 + x \equiv 5 \pmod{12}$

(iii) $4 - 7 \equiv x \pmod{12}$ **(iv)** $42 - x \equiv 8 \pmod{12}$

[8 marks]

1.5 A Modulo Six Clock

There is no particular reason why a modulo clock has to have twelve integers upon its face. Here is a modulo six clock;



For the modulo six clock the set of least residues is {0, 1, 2, 3, 4, 5}

1.6 Example

Solve the following congruence equation modulo 6.
Any answers should be given as elements from the set of least residues modulo 6.

$$3x + 14 \equiv 5 \pmod 6$$

Teaching Video : http://www.NumberWonder.co.uk/v9108/1.mp4

[6 marks]

1.7 Exercise

Marks Available : 50

Question 1

Working modulo 12, what are the following congruent to ?

(i) 29 **(ii)** $-\ 7$ **(iii)** 145

(iv) $47 + 21$ **(iv)** $3 - 19$ **(vi)** 5^3

[4 marks]

Question 2

(a) Write down the set of least residues modulo 4.

[1 mark]

(b) Working modulo 4, what are the following congruent to ?
Answers should be elements from the set of least residues modulo 4.

(i) 7^0 **(ii)** 7^1 **(iii)** 7^2

(iv) 7^3 **(v)** 7^4 **(vi)** 7^5

[3 marks]

(c) From the pattern suggested in part (b), and still working modulo 4, what are the following congruent to ?

(i) 7^{758} **(ii)** 7^{433} **(iii)** $7^{501} + 7^{383}$

[3 marks]

Question 3

Solve the following congruence equations modulo 8.
Answers should be given as elements from the set of least residues modulo 8.

(i) $6 + 4 \equiv x \pmod 8$ **(ii)** $3 + x \equiv 1 \pmod 8$

(iii) $4 - 19 \equiv x \pmod 8$ **(iv)** $37 - x \equiv 8 \pmod 8$

[8 marks]

Question 4

Solve the following congruence equation modulo 6.

Any answers should be given as elements from the set of least residues modulo 6.

$$2x + 11 \equiv 1 \pmod{6}$$

[6 marks]

Question 5

Consider integer addition modulo 5.

As any integer what-so-ever is congruent to an element in the set of least residues modulo 5, all possible modulo 5 additions can be captured in one simple table.

Here is that table;

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Highlighted is the addition, $3 + 4 \equiv 2 \pmod{5}$

Produce a similar table for multiplication modulo 5;

$\times_5$	0	1	2	3	4
0					
1					
2					
3					
4					

[4 marks]

Question 6

5! is said "5 factorial"

5! means $5 \times 4 \times 3 \times 2 \times 1$

Your calculator will tell you that 5! = 120

However, $5! \equiv 1 \pmod 7$ because $120 = 17 \times 7 + 1$

(a) Working modulo 7, what are the following congruent to ?

(i)	1!	**(ii)**	2!	**(iii)**	3!
(iv)	4!	**(v)**	5!	**(vi)**	6!
(vii)	7!	**(viii)**	8!	**(ix)**	9!

[3 marks]

(b) **(i)** From part (a), Lilibet conjectures that.

$n! \equiv 0 \pmod 7$ for $n \geqslant 7$ where $n \in \mathbb{Z}^+$

Lilibet is correct. Explain why.

[2 marks]

Question 7

(a) Working modulo 9, what are the following congruent to ?

(i)	13	**(ii)**	572	**(iii)**	334
(iv)	85507	**(v)**	1002001	**(vi)**	9994999

[3 marks]

(b) There is a quick "trick" for working out the answers to part (a)

Explain what this "trick" is and use it to determine the value of,

$$12345678987654321 \pmod 9$$

[2 marks]

Question 8
Find the remainder when $1! + 2! + 3! + 4! + ... + 100!$ is divided by 15.
In other words, find the value of,

$$1! + 2! + 3! + 4! + ... + 100! \pmod{15}$$

[5 marks]

Question 9
The serial number of a certain currency is 11 digits long.
The first 10 digits of the serial number are followed by a security check digit.
For the note to pass the security check, the 10 digit number will be congruent to the check digit modulo 9.
For each of these serial numbers, determine is they pass the security check.

(i) 51177875501 **(ii)** 88100245327

[2 marks]

Question 10
Determine the value of,

$$1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + ... + 100^2 \pmod{4}$$

[4 marks]

1.8 Answers

1.8.1 Solutions to 1.4 Exercise

(i)

$$6 + 9 \equiv x \pmod{12}$$
$$x \equiv 15 \pmod{12}$$
$$x \equiv 3 \pmod{12}$$

(ii)

$$10 + x \equiv 5 \pmod{12}$$
$$x \equiv 5 - 10 \pmod{12}$$
$$x \equiv -5 \pmod{12}$$
$$x \equiv 7 \pmod{12}$$

(iii)

$$4 - 7 \equiv x \pmod{12}$$
$$x \equiv -3 \pmod{12}$$
$$x \equiv 9 \pmod{12}$$

(iv)

$$42 - x \equiv 8 \pmod{12}$$
$$x \equiv 42 - 8 \pmod{12}$$
$$x \equiv 34 \pmod{12}$$
$$x \equiv 10 \pmod{12}$$

[8 marks]

1.8.2 Solution to 1.6 Example (Teaching Video)

Note : This is a “beginners” method with a premium placed on “understanding”

$$3x + 14 \equiv 5 \pmod{6}$$
$$3x \equiv 5 - 14 \pmod{6}$$
$$3x \equiv -9 \pmod{6}$$
$$3x \equiv 3,\ 9,\ 15,\ 21,\ 27,\ \ldots \pmod{6}$$
$$x \equiv 1,\ 3,\ 5 \pmod{6}$$

This could be more succinctly written as $x \equiv 1 \pmod{2}$

[6 marks]

1.8.3 Solutions to 1.7 Exercise

Answer 1

(i) $29 \equiv 5 \pmod{12}$

(ii) $-7 \equiv 5 \pmod{12}$

(iii) $145 \equiv 1 \pmod{12}$

(iv) $47 + 21 \equiv 68 \equiv 8 \pmod{12}$

(iv) $3 - 19 \equiv -16 \equiv 8 \pmod{12}$

(vi) $5^3 \equiv 125 \equiv 5 \pmod{12}$

[4 marks]

Answer 2

(a) Least residues modulo 4 = { 0, 1, 2, 3 }

[1 mark]

(b) **(i)** $7^0 \equiv 1 \pmod 4$

(ii) $7^1 \equiv 7 \equiv 3 \pmod 4$

(iii) $7^2 \equiv 49 \equiv 1 \pmod 4$

(iv) $7^3 \equiv 343 \equiv 3 \pmod 4$

(v) $7^4 \equiv 2401 \equiv 1 \pmod 4$

(vi) $7^5 \equiv 16807 \equiv 3 \pmod 4$

[3 marks]

(c) From the pattern observed in part (b) it would seem that,

$$7^{EVEN} \equiv 1 \pmod 4$$

$$7^{ODD} \equiv 3 \pmod 4$$

(i) $7^{758} \equiv 1 \pmod 4$

(ii) $7^{433} \equiv 3 \pmod 4$

(iii) $7^{501} + 7^{383} \equiv 3 + 3 \equiv 6 \equiv 2 \pmod 4$

[3 marks]

Answer 3

(i) $6 + 4 \equiv x \pmod 8$

$x \equiv 10 \pmod 8$

$x \equiv 2 \pmod 8$

(ii) $3 + x \equiv 1 \pmod 8$

$x \equiv 1 - 3 \pmod 8$

$x \equiv -2 \pmod 8$

$x \equiv 6 \pmod 8$

(iii) $4 - 19 \equiv x \pmod 8$

$x \equiv -15 \pmod 8$

$x \equiv 1 \pmod 8$

(iv) $37 - x \equiv 8 \pmod 8$

$x \equiv 37 - 8 \pmod 8$

$x \equiv 29 \pmod 8$

$x \equiv 5 \pmod 8$

[8 marks]

Answer 4

$$2x + 11 \equiv 1 \pmod 6$$
$$2x \equiv 1 - 11 \pmod 6$$
$$2x \equiv -10 \pmod 6$$
$$2x \equiv 2,\ 8,\ 14,\ \ldots \pmod 6$$
$$x \equiv 1,\ 4,\ 7,\ \ldots \pmod 6$$
$$x \equiv 1,\ 4 \pmod 6$$

This could be more succinctly written as $x \equiv 1 \pmod 3$

[6 marks]

Answer 5

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

[4 marks]

Answer 6

(a) **(i)** $1! \equiv 1 \pmod 7$

(ii) $2! \equiv 2 \pmod 7$

(iii) $3! \equiv 6 \pmod 7$

(iv) $4! \equiv 24 \equiv 3 \pmod 7$

(v) $5! \equiv 120 \equiv 1 \pmod 7$

(vi) $6! \equiv 720 \equiv 6 \pmod 7$

(vii) $7! \equiv 5040 \equiv 0 \pmod 7$

(viii) $8! \equiv 40320 \equiv 0 \pmod 7$

(ix) $9! \equiv 362880 \equiv 0 \pmod 7$

[3 marks]

(b) For $n \geqslant 7$, $n = 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times \ldots \times n$

As it contains a 7, it will divide by 7 and so be congruent to 0 modulo 7

[2 marks]

Answer 7

(a) **(i)** $13 \equiv 4 \pmod 9$ $\quad 1 + 3 = 4$

(ii) $572 \equiv 5 \pmod 9$ $\quad 5 + 7 + 2 = 14 \Rightarrow 1 + 4 = 5$

(iii) $334 \equiv 1 \pmod 9$ $\quad 3 + 3 + 4 = 10 \Rightarrow 1 + 0 = 1$

(iv) $3102 \equiv 6 \pmod 9$ $\quad 3 + 1 + 0 + 2 = 6$

(v) $1002001 \equiv 4 \pmod 9$ $\quad 1 + 0 + 0 + 2 + 0 + 0 + 1 = 4$

(vi) $9994999 \equiv 4 \pmod 9$ $\quad 9 + 9 + 9 + 4 + 9 + 9 + 9 = 58$

$\Rightarrow 5 + 8 = 13$

$\Rightarrow 1 + 3 = 4$

[3 marks]

(b) The answers can be obtained by summing the digits modulo 9, as shown above for the part (a) questions.

$$12345678987654321$$

$$\Rightarrow 2(1 + 2 + 3 + 4 + 5 + 6 + 7 + 8) + 9$$

$$= 2(\,(1 + 8) + (2 + 7) + (3 + 6) + (4 + 5)) + 9$$

$$= 2 \times 4 \times 9 + 9$$

$$\equiv 0 \pmod 9$$

[2 marks]

Answer 8

When $n \geqslant 5$, $n! \equiv 0 \pmod{15}$ because $n!$ then contains factors of both 3 and 5 and so contains a factor of 15.

$$1! + 2! + 3! + 4! + ... + 100! \pmod{15}$$

$$\equiv 1! + 2! + 3! + 4! + 0 + 0 + 0 + ... + 0 \pmod{15}$$

$$\equiv 1 + 2 + 6 + 24 \pmod{15}$$

$$\equiv 3 \pmod{15}$$

So the remainder is 3

[5 marks]

Answer 9

(i) For 51177875501

$$5 + 1 + 1 + 7 + 7 + 8 + 7 + 5 + 5 + 0 = 46$$

$$\Rightarrow 4 + 6 = 10$$

$$\Rightarrow 1 + 0 = 1$$

As 1 is the check digit, this serial number passes the security check.

(ii) For 88100245327

$$8 + 8 + 1 + 0 + 0 + 2 + 4 + 5 + 3 + 2 = 33$$

$$\Rightarrow 3 + 3 = 6$$

As 6 is not the check digit, this serial number does not pass.

[2 marks]

Answer 10

$1^2 \equiv 1 \pmod 4$

$2^2 \equiv 4 \equiv 0 \pmod 4$

$3^2 \equiv 9 \equiv 1 \pmod 4$

$4^2 \equiv 16 \equiv 0 \pmod 4$

$5^2 \equiv 25 \equiv 1 \pmod 4$

$6^2 \equiv 36 \equiv 0 \pmod 4$

...

To prove the pattern suggested by the above, show that any odd number squared is congruent to 1 modulo 4 and that any even number squared is congruent to 0 modulo 4, which is not difficult.

$$1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + \ldots + 100^2 \pmod 4$$

$$\equiv 1 + 0 + 1 + 0 + 1 + 0 + \ldots + 0 \pmod 4$$

$$\equiv 50 \pmod 4$$

$$\equiv 2 \pmod 4$$

[4 marks]

Lecture 2

University Undergraduate Lectures in Mathematics
A First Year Course
Group Theory I

2.1 Properties of Groups

All possible additions modulo 5 can be summarised by the table;

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

This is a well known group called the cyclic group, C_5

It is alive with patterns such as,

- In any given row each of the five possible least residues occur once and once only
- In any given column each of the five possible least residues occur once and once only

Taken together this pattern is referred to as the Latin square property of a group.
All groups have this Latin square property.

Another of the key ideas behind what makes this a group are the facts that,

◊ There is a defined set, $G = \{ 0, 1, 2, 3, 4 \}$

◊ There is a binary operation defined upon G, addition modulo 5

A Binary Operation

A binary operation on a set is a calculation that combines two elements of the set to produce another element of the set.

To be a group there must be an element that "does nothing", in this case the number zero. When zero is added on to any of the other elements it leaves them unchanged. This special element is called the identity element, *e*.

Furthermore, to be a group, each element must have an inverse.
The inverse of 2, for example, is 3 because when 2 and 3 are combined in either order, the result is the identity element.

$$2 + 3 \equiv 0 \pmod 5 \qquad \text{and} \qquad 3 + 2 \equiv 0 \pmod 5$$

There are two other conditions that must be satisfied.
One is termed “Closure” which means that under the binary operation of the group it's not possible to obtain an answer that is outside of the group.
The final condition is that “Associativity” holds.
Briefly, this requires that for any three elements in the group, a, b, and c, where the brackets are placed must make no difference.

That is, $a + (b + c) \equiv (a + b) + c \pmod 5$

2.2 Dismissed, then Reformed

All possible multiplications modulo 5 can be summarised by the table;

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

This is not a group because, for example, the Latin square property does not hold.
However, if zero is removed from the set of least residues modulo 5, it is a group !

2.3 Example

Prove that $G = \{1, 2, 3, 4\}$ under multiplication modulo 5 is a group.

Teaching Video: http://www.NumberWonder.co.uk/v9108/2.mp4

[6 marks]

2.4 Exercise

Marks Available : 40

Question 1

The set G = { 1, 5, 7, 11, 13, 17 } forms a group under multiplication modulo 18. Natasha has constructed most of its Cayley table;

$\times_{18}$	1	5	7	11	13	17
1	1	5		11	13	17
5	5	7	17	1		13
7		17		5	1	11
11	11	1	5	13		7
13	13		1		7	5
17	17	13	11	7	5	1

(i) Complete the Cayley table for Natasha.

[2 marks]

(ii) What is this group's identity element ?

[1 mark]

(iii) What is the inverse of the number 5 ?

[1 mark]

(iv) What is the inverse of the number 17 ?

[1 mark]

Question 2

A binary operation on integers, $*$, is defined as $x * y = x^2 y$

Determine the value of,

(i) $5 * 6$ **(ii)** $6 * 5$

[2 marks]

Question 3

Walter is investigating if the set $G = \{ 1, 3, 7, 9 \}$ forms a group under multiplication modulo 12 and has started to try and construct a Cayley table;

$\times_{12}$	1	3	7	9
1	1	3	7	9
3	3	9		
7	7		1	3
9	9		3	

(i) Complete the table.

[2 marks]

(ii) Is the closure property satisfied ?

[1 mark]

(iii) Give at least one reason why a group has not been formed.

[1 mark]

Question 4

A binary operation on $\mathbb{Z}$ is defined by $a * b = ab + 1$

($\mathbb{Z}$ is the set of integers, $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$)

(a) Determine the value of,

(i) $4 * 7$ **(ii)** $(-3) * 5$

[2 marks]

(b) By considering the integers 2, 3 and 4 show that $*$ is not associative.

[2 marks]

Question 5

The set $G = \{ 0, 1, 2, 4, 5, 6 \}$ forms a group under the binary operation,

$$x \circ y = x + y + 2xy \pmod 7$$

Sebastian has started to constructed this group's Cayley table;

$\circ$	**0**	**1**	**2**	**4**	**5**	**6**
0		**1**				
1		**4**				
2						
4					**0**	**2**
5						
6					**1**	

(i) Complete the Cayley table for Sebastian.

[3 marks]

(ii) What is this group's identity element ?

[1 mark]

(iii) What is the inverse of the number 5 ?

[1 mark]

(iv) What is the inverse of the number 1 ?

[1 mark]

(v) Which element, other than the identity element, is self-inverse ?

[1 mark]

Question 6

Let G be the set of (positive) odd numbers.

Let $\circ$ be the binary operation acting on G, $x \circ y = x^2 y$

Prove that G is closed under $\circ$

[2 marks]

Question 7

Let $G = \{ 1, 2, 3, 4, 5 \}$

Under an unknown binary operation, $\otimes$, the following table is obtained.

$\otimes$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	2	5	1
4	4	5	1	2	3
5	5	3	4	1	2

Tom claims, "As the table has the Latin square property it is a group".
Paul, however, is doubtful and sets about proving Tom's claim is false.

(a) Show that the following two calculations yield different answers;

(i) $2 \otimes (5 \otimes 3)$ **(ii)** $(2 \otimes 5) \otimes 3$

[2 marks]

(b) What property does part (a) show the table not to have ?

[1 mark]

Whilst all Cayley tables for a group have the Latin square property, this question shows that not all tables with the Latin square property are groups. Latin squares that are not groups are termed quasigroups.

Question 8

The operation $\circ$ is defined by $x \circ y = xy + x$ where $x, y \in \mathbb{R}$

By considering associativity, show that $\mathbb{R}$ does not form a group under $\circ$

[4 marks]

Question 9
Here is the first half of a proof that all Cayley group tables are Latin squares.

It begins with the assumption that there exists a row in a group's Cayley table in which the same element occurs twice.
So, given two distinct elements, x and y, in row a the situation is;

$\circ$	…	x	…	y	…
…	…	…	…	…	…
a	…	$a\circ x$	…	$a\circ y$	…
…	…	…	…	…	…

And under the assumption that the same element occurs twice,

$$a \circ x = a \circ y$$

$$a^{-1} \circ (a \circ x) = a^{-1} \circ (a \circ y) \qquad \text{Every element in a group has an inverse}$$

$$(a^{-1} \circ a) \circ x = (a^{-1} \circ a) \circ y \qquad \text{A group has associativity}$$

$$e \circ x = e \circ y \qquad e \text{ is the identity element}$$

$$x = y$$

But this contradicts the starting assumption that x and y are distinct elements.
$\therefore$ the same element cannot occur twice in any row in a group Cayley table.

Complete the proof by showing that an element cannot occur twice in any column.

[2 marks]

Question 10

(a) Given that $f(x) = \dfrac{3x - 1}{7x - 2}$, show that $ff(x) = \dfrac{2x - 1}{7x - 3}$

[3 marks]

(b) Given that, as before, $f(x) = \dfrac{3x - 1}{7x - 2}$, show that $fff(x) = x$

[3 marks]

(c) With $G = \{ f(x),\ ff(x),\ fff(x) \}$ and the binary operation $\circ$ being composition of functions, a group if formed.
Here are a couple of ways of writing out the Cayley table for this group;

$\circ$	$f(x)$	$ff(x)$	$fff(x)$
$f(x)$	$ff(x)$	$fff(x)$	$f(x)$
$ff(x)$	$fff(x)$	$f(x)$	$ff(x)$
$fff(x)$	$f(x)$	$ff(x)$	$fff(x)$

$\circ$	$\frac{3x-1}{7x-2}$	$\frac{2x-1}{7x-3}$	x
$\frac{3x-1}{7x-2}$	$\frac{2x-1}{7x-3}$	x	$\frac{3x-1}{7x-2}$
$\frac{2x-1}{7x-3}$	x	$\frac{3x-1}{7x-2}$	$\frac{2x-1}{7x-3}$
x	$\frac{3x-1}{7x-2}$	$\frac{2x-1}{7x-3}$	x

(i) What is the identity element of this group ?

[1 mark]

(ii) What is $fff(x) \circ ff(x)$?

[1 mark]

(iii) What is the inverse of the element $ff(x)$?

[1 mark]

2.5 Answers

2.5.1 Solution to 2.3 Example (Teaching Video)

Prove $G = \{ 1, \ 2, \ 3, \ 4 \}$ under multiplication modulo 5 is a group.

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Identity: For this group, 1 is the identity element, the element that "does nothing" under the binary operation of multiplication modulo 5.

Closure : As the table shows all possible multiplications it can be seen that no number can occur as an answer that's not an element of $G = \{ 1, 2, 3, 4 \}$.

Inverse : Each element has a unique inverse. 2 and 3 are each the other's inverse and 4 is it's own inverse as is 1.

$2 \times 3 \equiv 3 \times 2 \equiv 1 \pmod 5 \quad 4 \times 4 \equiv 1 \pmod 5$

Associativity : This is a property inherited from of multiplication of integers.

2.5.2 Solutions to 2.4 Exercise

Answer 1

(i)

$\times_{18}$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

[2 marks]

(ii) The identity element is 1

[1 mark]

(iii) The inverse of 5 is 11 because $5 \times 11 = 1 \pmod{18}$

[1 mark]

(iv) The inverse of 17 is 17 because $17 \times 17 = 1 \pmod{18}$

[1 mark]

Answer 2

$x * y = x^2 y$

(i) $5 * 6 = 5^2 \times 6 = 150$

(ii) $6 * 5 = 6^2 \times 5 = 180$

[2 marks]

Answer 3

(i)

$\times_{12}$	1	3	7	9
1	1	3	7	9
3	3	9	9	3
7	7	9	1	3
9	9	3	3	9

[2 marks]

(ii) Yes, the closure property is satisfied.

[1 mark]

(iii)
- The Latin square property does not hold.
- Two of the elements, the 3 and the 9, do not have an inverse.

[1 mark]

Answer 4

$a * b = ab + 1$

(a) **(i)** $4 * 7 = 4 \times 7 + 1$

$= 29$

(ii) $(-3) * 5 = (-3) \times 5 + 1$

$= -14$

[2 marks]

(b) $2 * (3 * 4) = 2 * (3 \times 4 + 1)$

$= 2 * 13$

$= 2 \times 13 + 1$

$= 27$

$(2 * 3) * 4 = (2 \times 3 + 1) * 4$

$= 7 * 4$

$= 7 \times 4 + 1$

$= 29$

Thus $2 * (3 * 4) \neq (2 * 3) * 4$

$\therefore$ $*$ is not associative ☐

[2 marks]

Answer 5

(i)

$\circ$	0	1	2	4	5	6
0	0	1	2	4	5	6
1	1	4	0	6	2	5
2	2	0	5	1	6	4
4	4	6	1	5	0	2
5	5	2	6	0	4	1
6	6	5	4	2	1	0

[3 marks]

(ii) The identity element is 0

[1 mark]

(iii) The inverse of 5 is 4

[1 mark]

(iv) The inverse of 1 is 2

[1 mark]

(v) Other than 0, the self-inverse element is 6

[1 mark]

Answer 6

Method 1 :

$$\begin{aligned} x \circ y &= x^2 y \\ odd \circ odd &= odd^2 \times odd \\ &= odd \times odd \\ &= odd \end{aligned}$$

So, when any two elements from G are combined the result

is an element from G which is what is means to be closed ☐

Method 2 :

Let the two odd numbers be $2n + 1$ and $2m + 1$

$$\begin{aligned} (2n + 1) \circ (2m + 1) &= (2n + 1)^2 (2m + 1) \\ &= 2\left(4m\,n^2 + 4nm + m + 2\,n^2 + 2n\right) + 1 \\ &= 2k + 1, \text{ another odd number} \end{aligned}$$

$\therefore$ G is closed under $\circ$

[2 marks]

Answer 7

(a) From the Cayley table provided,

$\otimes$	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**
2	**2**	**1**	**5**	**3**	**4**
3	**3**	**4**	**2**	**5**	**1**
4	**4**	**5**	**1**	**2**	**3**
5	**5**	**3**	**4**	**1**	**2**

(i) $2 \otimes (5 \otimes 3) = 2 \otimes 4$

$= 3$

(ii) $(2 \otimes 5) \otimes 3 = 4 \otimes 3$

$= 1$

[2 marks]

(b) The table does not have associativity and so is not of a group.

[1 mark]

Answer 8

$x \circ y = xy + x$

Let's check to see if associativity holds.

In other words, for any three elements of G, say a, b and c, is it true that,

$a \circ (b \circ c) = (a \circ b) \circ c$?

$$\begin{aligned} \text{LHS} &= a \circ (b \circ c) \\ &= a \circ (bc + b) \\ &= a(bc + b) + a \\ &= abc + ab + a \end{aligned} \qquad \begin{aligned} \text{RHS} &= (a \circ b) \circ c \\ &= (ab + a) \circ c \\ &= (ab + a)c + (ab + a) \\ &= abc + ac + ab + a \end{aligned}$$

As LHS $\neq$ RHS the proposed group lacks associativity and so is not a group under the binary operation $\circ$.

[4 marks]

Answer 9
Assume there exists a column in a Cayley table in which the same element occurs twice. Given two distinct elements, *p* and *q*, in column *b* the situation is;

$\circ$	...	$\boldsymbol{b}$	...
...	...	...	...
$\boldsymbol{p}$	...	$\boldsymbol{p \circ b}$	...
...	...	...	...
$\boldsymbol{q}$	...	$\boldsymbol{q \circ b}$	...
...	...	...	...

Under the assumption that the same element occurs twice,

$$p \circ b = q \circ b$$

$$(p \circ b) \circ b^{-1} = (q \circ b) \circ b^{-1} \qquad \text{Every element in a group has an inverse}$$

$$p \circ (b \circ b^{-1}) = q \circ (b \circ b^{-1}) \qquad \text{A group has associativity}$$

$$p \circ e = q \circ e \qquad e \text{ is the identity element}$$

$$p = q$$

But this contradicts the starting assumption that *p* and *q* are distinct elements.
∴ the same element cannot occur twice in any column in a group's Cayley table.

The two parts together prove that all group Cayley tables will be Latin squares.

[2 marks]

Answer 10

(a)

$$ff(x) = f\left(\frac{3x-1}{7x-2}\right)$$

$$= \frac{3\left(\frac{3x-1}{7x-2}\right) - 1}{7\left(\frac{3x-1}{7x-2}\right) - 2}$$

$$= \frac{9x - 3 - 7x + 2}{21x - 7 - 14x + 4}$$

$$= \frac{2x-1}{7x-3} \qquad \square$$

[3 marks]

(b)

$$fff(x) = ff\left(\frac{3x-1}{7x-2}\right)$$

$$= f\left(\frac{2x-1}{7x-3}\right)$$

$$= \frac{3\left(\frac{2x-1}{7x-3}\right) - 1}{7\left(\frac{2x-1}{7x-3}\right) - 2}$$

$$= \frac{6x - 3 - 7x + 3}{14x - 7 - 14x + 6}$$

$$= \frac{-x}{-1}$$

$$= x \qquad \square$$

[3 marks]

(c) **(i)** The identity element is $fff(x)$ because $fff(x) = x$

[1 mark]

(ii) $fff(x) \circ ff(x) = e \circ ff(x)$ $\qquad$ e is the identity

$$= ff(x)$$

[1 mark]

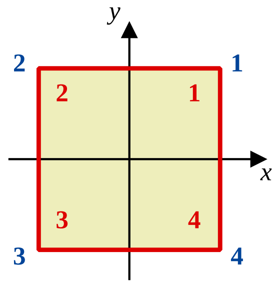
(iii) The inverse of $ff(x)$ is $f(x)$ because,

$$ff(x) \circ f(x) = f(x) \circ ff(x) = e$$

[1 mark]

3.1 The Square

To investigate the symmetries of a square, it can be placed with its centre at the origin of a Cartesian plane. The four corners of the square can be numbered to note in which quadrants they lie when in this "starting position".

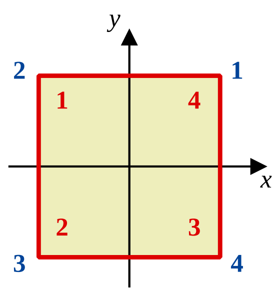


The quadrants are numbered from 1 to 4 in blue
The corners of the square are numbered from 1 to 4 in red

The first thing to do is "do nothing" !
Traditionally this is called the identity operation and is designated, *e*

3.2 Rotational Symmetry

More interesting, is to define the operation *r* as "rotate 90°"
(This will be anticlockwise, of course)
After applying *r* the situation will look like this;



Using permutation notation, $r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

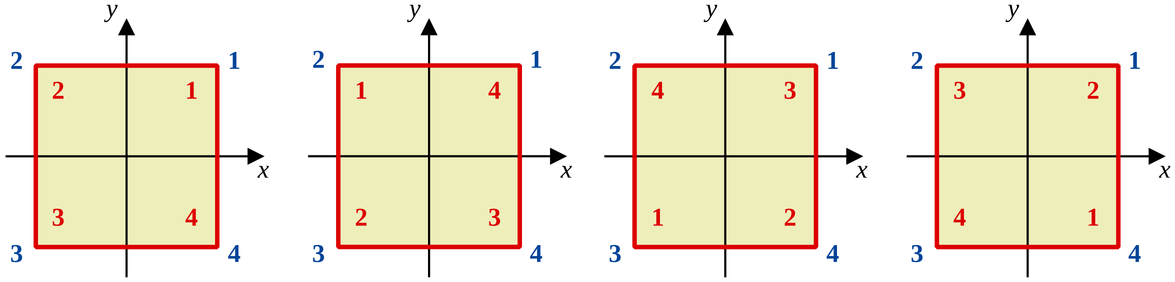
The second row shows in which quadrant each vertex is now located.

Two other symmetries of the square are "rotate 180°" and "rotate 270" which can be defined as r^2 and r^3 respectively.

Thus, for example, r^2 means "rotate 90" and then "rotate 90°" again.

Notice that $r^4 = e$

Here is a summary of the discussion so far;



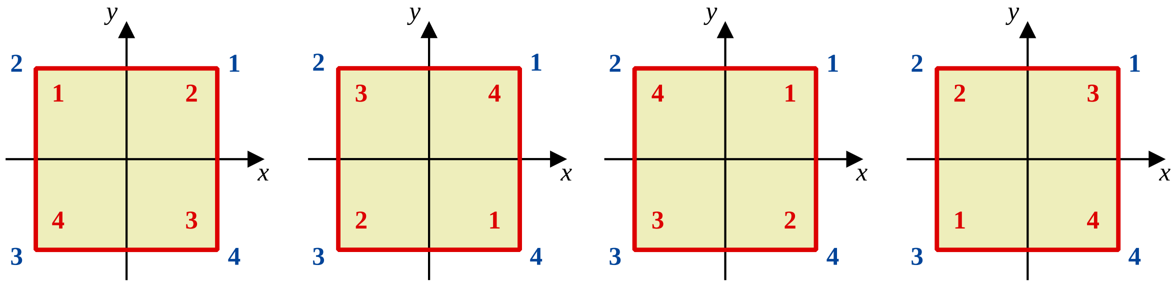
$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ $r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ $r^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ $r^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

3.3 Mirror Symmetry

In addition to rotational symmetry, a square has mirror symmetry.

By definition let
- ◊ y be "reflection in the y-axis"
- ◊ x be "reflection in the x-axis"
- ◊ p be "reflection in the line with positive gradient, $y = x$"
- ◊ n be "reflection in the line with negative gradient, $y = -x$"

This adds four more diagrams and permutations to the proceedings;



$y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ $x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ $n = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

Notice that, $y^2 = x^2 = p^2 = q^2 = e$

3.4 The Order of a Group

In total, eight symmetries of the square have been identified.
These will form a group of order 8, and the Cayley table for this group will be an 8 by 8 grid. The symmetries can thus be combined under the binary operation "followed by" in sixty-four different ways.
Foe example, one of the sixty-four is "rotation of 90° followed by reflection in x-axis".

The Order of a Group
The order of a group is simply the number of elements in the set upon which the binary operation acts.

3.5 An Example of Combining Symmetries

The result of combing two of the square's symmetries can be determined mathematically by using permutation notation.

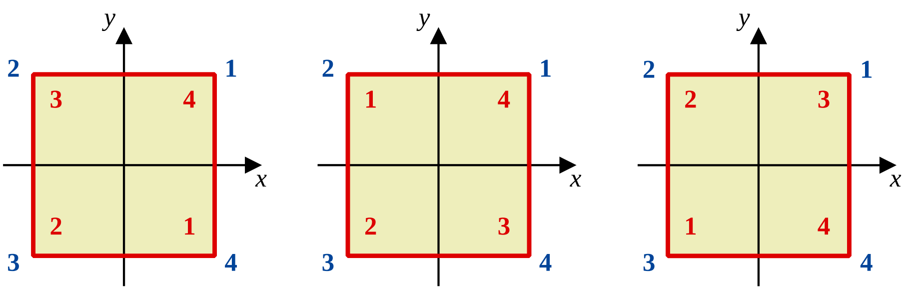
Show for a square that, using permutations, a rotation of 90° followed by a reflection in the x-axis is equivalent to a reflection in the line $y = -x$

Teaching Video: http://www.NumberWonder.co.uk/v9108/3.mp4

Solution :

The three symmetries involved and their associated permutations are;

- x is a reflection in the x-axis
- r is a rotation of 90°
- n is a reflection in the line $y = -x$



$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ $r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ $n = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

[4 marks]

3.6 The Cayley Table for a Square

Working through all possible pairs of ways of combining the symmetries of the square gives rise to the following Cayley table.

top

then tail

$*$	e	r	r^2	r^3	y	x	p	n
e	e	r	r^2	r^3	y	x	p	n
r	r	r^2	r^3	e	n	p	y	x
r^2	r^2	r^3	e	r	x	y	n	p
r^3	r^3	e	r	r^2	p	n	x	y
y	y	p	x	n	e	r^2	r^3	r
x	x	n	y	p	r^2	e	r	r^3
p	p	x	n	y	r	r^3	e	r^2
n	n	y	p	x	r^3	r	r^2	e

This is a well known group called the dihedral group, D_4

It's alive with patterns such as,

- In any given row the eight possible symmetries occur once and once only
- In any given column the eight possible symmetries occur once and once only

Taken together this pattern is referred to as the Latin square property of a group. All groups have this Latin square property buy not all Latin squares are groups.

In reading the Cayley table notice that $x * r$ means do r first which is the r in the red row across the top of the table, then do x second which is the x in the green column down the left hand side of the table. Top then tail.

Notice that whereas $x * r = n,\ r * x = p$. That is $xr \neq rx$.

3.7 Exercise

Marks Available : 40

Question 1

Two permutations are

$$v = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \text{ and } w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

(i) Determine the composite permutation $v \circ w$

[2 marks]

(ii) Determine the composite permutation $w \circ v$

[2 marks]

(iii) For v determine the inverse permutation, v^{-1}

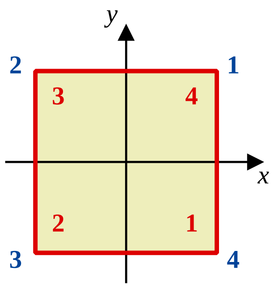
[2 marks]

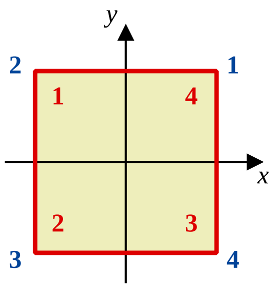
Question 2

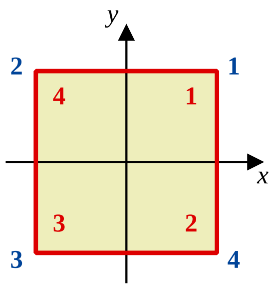
Show for a square that, using permutations, a reflection in the x-axis followed by a rotation of 90° is equivalent to a reflection in the line $y = x$

In answering this question label the symmetries as follows;

- x is a reflection in the x-axis
- r is a rotation of 90°
- p is a reflection in the line $y = x$



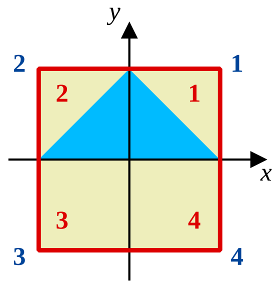




$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ $r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

[4 marks]

Question 3



The patterned square shown only has the symmetry, reflection in the *y*-axis, *y*, in addition to the “do nothing” identity, *e*.

(i) Complete the Cayley table for the group formed by $G = \{ e, y \}$ under the binary operation of composition of symmetries.

$*$	e	y
e		
y		

[1 mark]

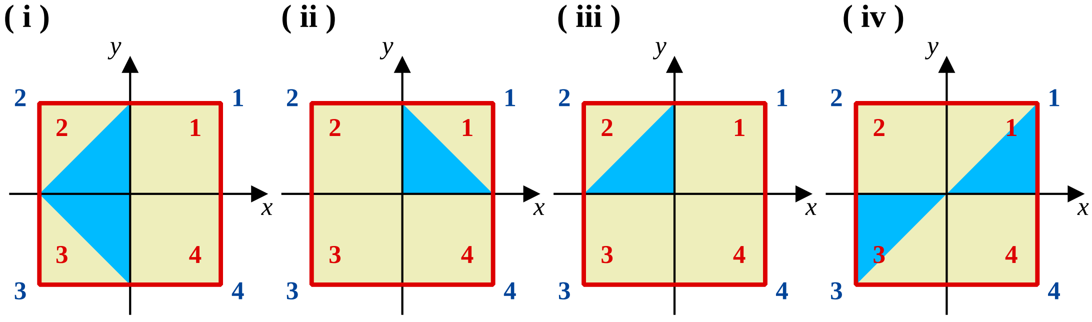
(ii) The part (i) group is a subgroup of the group of symmetries of the (unpatterned) square.
Here it is;

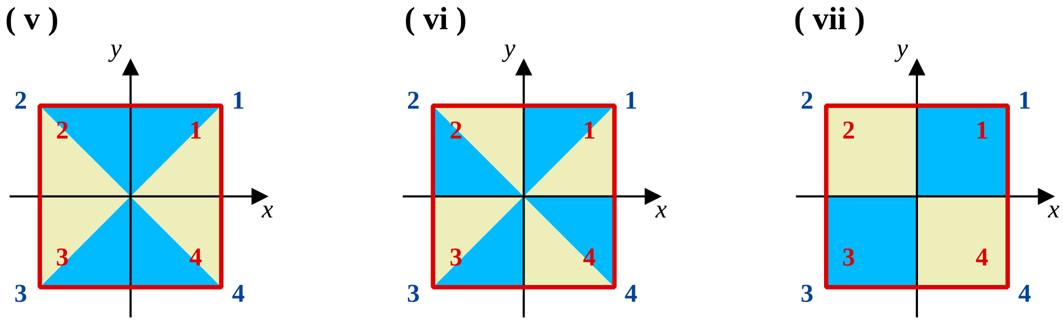
$*$	e	r	r^2	r^3	y	x	p	n
e	e	r	r^2	r^3	y	x	p	n
r	r	r^2	r^3	e	n	p	y	x
r^2	r^2	r^3	e	r	x	y	n	p
r^3	r^3	e	r	r^2	p	n	x	y
y	y	p	x	n	e	r^2	r^3	r
x	x	n	y	p	r^2	e	r	r^3
p	p	x	n	y	r	r^3	e	r^2
n	n	y	p	x	r^3	r	r^2	e

What is the order of this subgroup ?

[1 mark]

Question 4
Each of the following patterned squares gives rise to a symmetry group that is a subgroup of the symmetry group of the (unpatterned) square.
For each patterned square, construct its associated Cayley table,





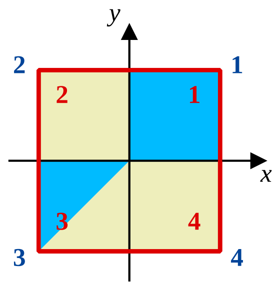
[14 marks]

Question 5

From questions 3 and 4, you should have unearthed that the symmetry group of the square, (which is of order 8), has five subgroups of order 2, and three subgroups of order 4.

The identity element on its own can also be considered a subgroup corresponding to a patterned square with no symmetry, such as the example shown below.

It adds one subgroup of order 1 to the list of subgroups of the (unpatterned) square.



Finally, the whole group is considered to be a subgroup of itself.

That concession adds one subgroup or order 8.

Here is a summary of all subgroups found;

Subgroup	Order	Number Found
$\{e\}$	1	1
$\{e, x\}, \{e, y\},$ $\{e, p\}, \{e, n\},$ $\{e, r^2\}$	2	5
$\{e, r, r^2, r^3\}$ $\{e, r^2, x, y\}$ $\{e, r^2, p, n\}$	4	3
$\{e, r, r^2, r^3, x, y, p, n\}$	8	1

There is a £5,000,000 prize for the person who finds a subgroup of the symmetries of a square of order 3, 5, 6 or 7. It can never be claimed !

What rule does the table of results suggest holds between the order of a group and the order of its subgroups ?

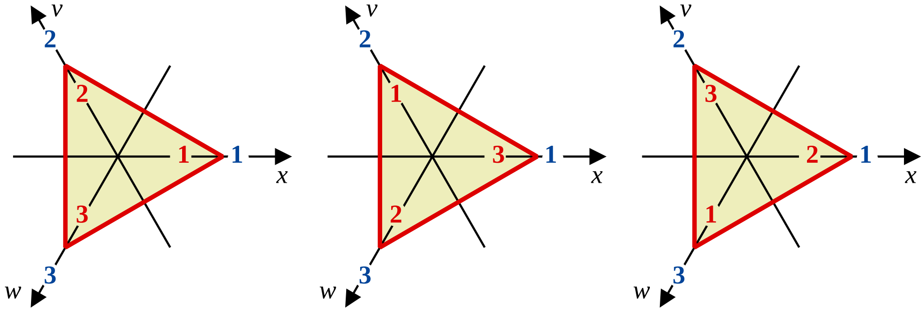
This rule is called Lagrange's Theorem.

[2 marks]

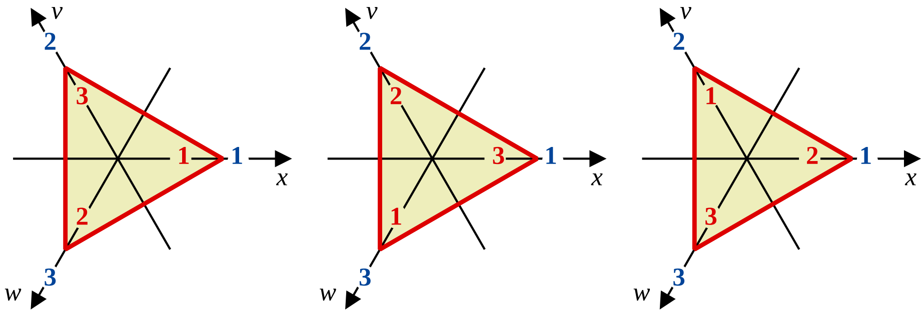
Question 6

The diagram shows the six symmetries of an equilateral triangle where

- ◊ e is "do nothing"
- ◊ r is rotation of 120°
- ◊ r^2 is rotation of 240°
- ◊ x is "reflection in the x-axis"
- ◊ v is "reflection in the v-axis"
- ◊ w is "reflection in the w-axis"



$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\quad r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\quad r^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$



$x = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\quad v = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\quad w = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Construct a Cayley table for the group of symmetries of the equilateral triangle

$*$	e	r	r^2	x	v	w
e						
r						
r^2						
x						
v						
w						

[6 marks]

Question 7

For the square, the following table of all possible subgroups was constructed,

Subgroup	Order	Number Found
$\{e\}$	1	1
$\{e, x\}$, $\{e, y\}$, $\{e, p\}$, $\{e, n\}$, $\{e, r^2\}$	2	5
$\{e, r, r^2, r^3\}$ $\{e, r^2, x, y\}$ $\{e, r^2, p, n\}$	4	3
$\{e, r, r^2, r^3, x, y, p, n\}$	8	1

Construct a similar table for all possible subgroups of the equilateral triangle.

[6 marks]

3.8 Answers

3.8.1 Solution to 3.5 An Example of Combining Symmetries (Teaching Video)

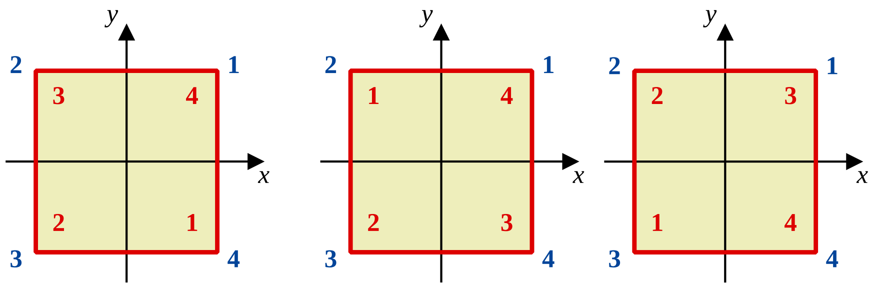
Question :

Show for a square that, using permutations, a rotation of 90° followed by a reflection in the x-axis is equivalent to a reflection in the line $y = -x$

Solution :

The three symmetries involved and their associated permutations are;

- x is a reflection in the x-axis
- r is a rotation of 90°
- n is a reflection in the line $y = -x$



$$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \qquad r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad n = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

So, the question is asking that it be shown that, $x * r = n$

(Take care over getting this the correct way round !)

$$\begin{aligned} \text{LHS} &= x * r \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \\ &= n \\ &= \text{RHS} \qquad \square \end{aligned}$$

Thus, a rotation of 90° followed by a reflection in the x-axis is indeed equivalent to a reflection in the line $y = -x$

[4 marks]

3.8.2 Solutions to 3.7 Exercise

Answer 1

(i)

$$v \circ w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$$

[2 marks]

(ii)

$$w \circ v = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$$

[2 marks]

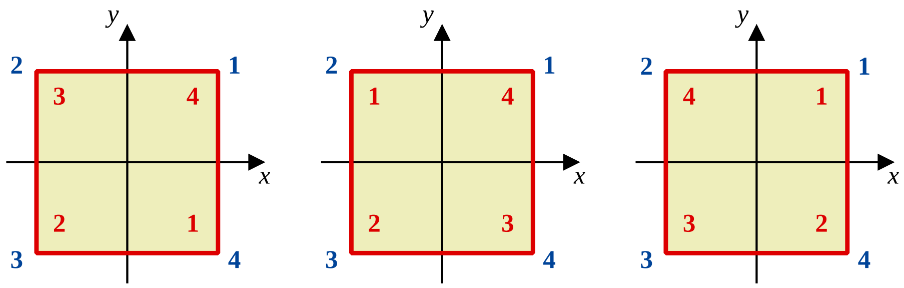
(iii)

$$v^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

[2 marks]

Answer 2



$$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \qquad r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Note that reflection in the x-axis, x, followed by a rotation of 90°, r is $r \circ x$
So, the question is requesting a proof that $r \circ x = p$

$$\text{LHS} = r \circ x$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$= \text{RHS} \qquad \square$$

Thus, reflection in the x-axis followed by rotation of 90° is indeed equivalent to a reflection in the line $y = x$

[4 marks]

Answer 3

(i)

$*$	e	y
e	e	y
y	y	e

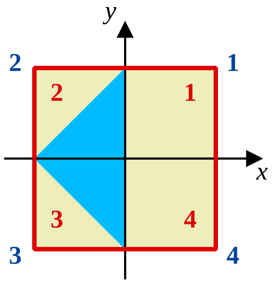
[1 mark]

(ii) This subgroup is of order 2

[1 mark]

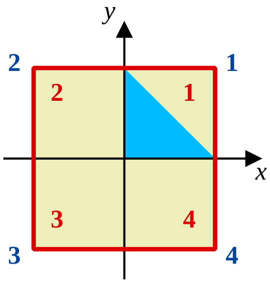
Answer 4

(i)



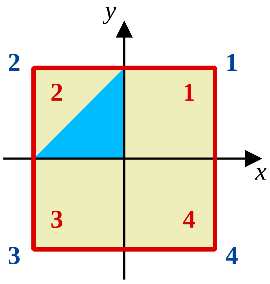
$*$	e	x
e	e	x
x	x	e

(ii)



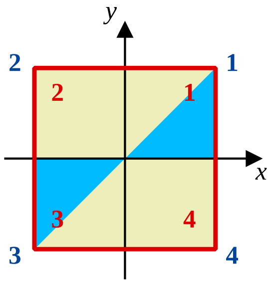
$*$	e	p
e	e	p
p	p	e

(iii)



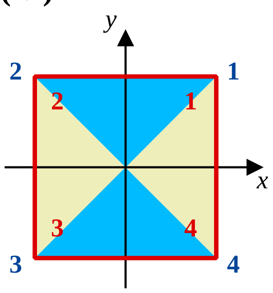
$*$	e	n
e	e	n
n	n	e

(iv)



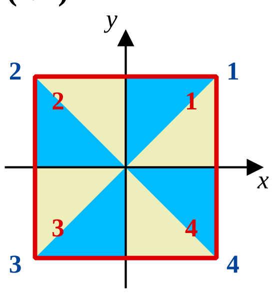
$*$	e	r^2
e	e	r^2
r^2	r^2	e

(v)



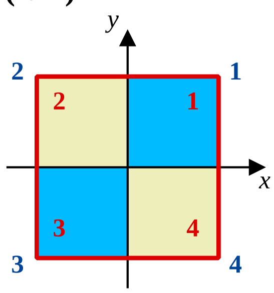
$*$	e	r^2	x	y
e	e	r^2	x	y
r^2	r^2	e	y	x
x	x	y	e	r^2
y	y	x	r^2	e

(vi)



$*$	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

(vii)



$*$	e	r^2	p	n
e	e	r^2	p	n
r^2	r^2	e	n	p
p	p	n	e	r^2
n	n	p	r^2	e

[14 marks]

Answer 5

Lagrange's Theorem
If H is a subgroup of a finite group G, the order of H divides the order of G.

A proof of this is a highlight of a first course in Group Theory at University. Historically it was first proven by Cauchy in 1844, about 30 years before Lagrange's major contributions to the subject.

[2 marks]

Answer 6

$*$	e	r	r^2	x	v	w
e	e	r	r^2	x	v	w
r	r	r^2	e	w	x	v
r^2	r^2	e	r	v	w	x
x	x	v	w	e	r	r^2
v	v	w	x	r^2	e	r
w	w	x	v	r	r^2	e

[6 marks]

Answer 7

Subgroup	Order	Number Found
$\{e\}$	1	1
$\{e, x\}, \{e, v\}, \{e, w\}$	2	3
$\{e, r, r^2\}$	3	1
$\{e, r, r^2, x, v, w\}$	6	1

[6 marks]

4.1 Generators

As the groups being dealt with get larger, a certain type of subgroup can be found by exploring the use of the groups elements as generators.

Any element, a, from a group $(G, *)$ can be selected as a generator.

The subgroup $(H, *)$ generated by a, is then $\langle a \rangle = H = \{a, a^2, a^3, a^4, \ldots\}$.

Once a term is found for which $a^k = e$, the generation halts.

Then $\langle a \rangle = H = \{a, a^2, a^3, a^4, \ldots, e\}$

The type of subgroup found in this way is termed a cyclic subgroup.

4.2 Example

$*$	e	r	r^2	r^3	y	x	p	n
e	e	r	r^2	r^3	y	x	p	n
r	r	r^2	r^3	e	n	p	y	x
r^2	r^2	r^3	e	r	x	y	n	p
r^3	r^3	e	r	r^2	p	n	x	y
y	y	p	x	n	e	r^2	r^3	r
x	x	n	y	p	r^2	e	r	r^3
p	p	x	n	y	r	r^3	e	r^2
n	n	y	p	x	r^3	r	r^2	e

For the group D_4 find $\langle r^3 \rangle$, the subgroup generated by the element r^3

Teaching Video: http://www.NumberWonder.co.uk/v9108/4.mp4

[3 marks]

4.3 Order of Elements

The group of symmetries of the square, D_4, is of order 8.

This can be written as $|D_4| = 8$

The same word is also applied to the elements of a set being used as a group.

The Order of an Element

The order of an element a in a group $(G, *)$ with identity e is the smallest positive integer k such that $a^k = e$

For example, in the group D_4, the element r has order 4 because $r^4 = e$ which corresponds to four 90° rotations of a square take it back to its starting position. This could be written as $|r| = 4$

4.4 Cyclic groups

Sometimes, but not always, an element in a group generates the entire group. Such a group is termed cyclic.

Cyclic Groups

$(G, *)$ is cyclic if and only if there exists an element a such that $|a| = |G|$
This element is termed a generator of the group.

Equivalently, a cyclic group is a group in which every element can be written in the form a^k, where a is the group generator and k is a positive integer.

Geometrically, in two dimensions, cyclic groups correspond to figures that have rotational symmetry and no mirror symmetry with the exception of a figure that only has a single mirror symmetry.

4.5 A Divisibility Restriction

Just as Lagrange's theorem restricted the possible orders of subgroup of any given group, the possible order of elements of any given group is restricted.

Possible Orders of Elements

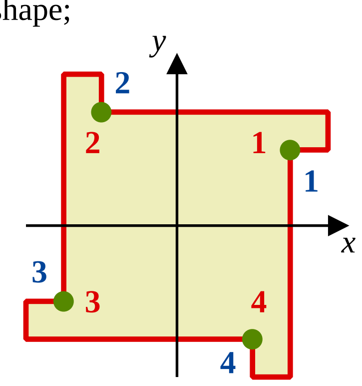
If $(G, *)$ has a finite number of elements, then, for every $a \in G$, the order of a divides the order of G. In other words, $|a|$ divides $|G|$

4.6 Exercise

Marks Available: 50

Question 1

Consider the following shape;



(i) Does the shape have any lines of mirror symmetry ?

[1 mark]

(ii) Does the shape have any rotational symmetry ?

[1 mark]

(iii) Will the symmetry group for this shape be cyclic under composition of symmetries ?

[1 mark]

(iv) In two line permutation notation, a symmetry of this shape is described as,

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

What symmetry of the shape does this correspond to ?

[1 mark]

(v) What is the order of the element a ?

[1 mark]

(vi) Produce a Cayley table of $\langle a \rangle$, the subgroup generated by a

[2 marks]

Question 2

The group shown is for addition modulo 12 on the set of least residues modulo 12;

$+_{12}$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

(i) Complete the table below;

Element	Subgroup Generated	Element's Order
0	$\langle 0 \rangle = \{0\}$	1
1		
2		
3		
4		
5		
6		
7		
8		
9		
10	$\langle 10 \rangle = \{0, 2, 4, 6, 8, 10\}$	6
11	$\langle 11 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$	12

[6 marks]

(ii) Is the group cyclic ?
Justify your answer.

[2 marks]

Question 3

G has elements $\{e,\ a,\ a^2,\ a^3,\ b,\ ba,\ b\,a^2,\ b\,a^3\}$ under a binary operation $*$ with Cayley table given by;

$*$	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	a^2	a^3	e	a
ba	ba	ba^2	ba^3	b	a	a^2	a^3	e
ba^2	ba^2	ba^3	b	ba	e	a	a^2	a^3
ba^3	ba^3	b	ba	ba^2	a^3	e	a	a^2

(i) State the order of the group.

[1 mark]

(ii) State the order of a and the order of b.

[2 marks]

(iii) What is $b\ *\ ba$?

[1 mark]

(iv) State the inverse of ba^2

[1 mark]

(v) Find and list the elements of a subgroup of order 4

[1 mark]

(vi) State the orders of the subgroups that Lagrange's theorem states can not exist for this group.

[1 mark]

Question 4
Further A-Level Examination question from June 2017, FP3, Q4a (OCR)

The composition table for a group G of order 6 is given below.

	a	***b***	***c***	***d***	***e***	***f***
a	c	f	e	b	a	d
b	f	a	d	e	b	c
c	e	d	a	f	c	b
d	b	e	f	c	d	a
e	a	b	c	d	e	f
f	d	c	b	a	f	e

(i) State the identity element.

[1 mark]

(ii) State the order of each element.

[3 marks]

(iii) Write the inverse of each element.

[3 marks]

(iv) Determine whether G is cyclic.

[2 marks]

(v) List all the proper subgroups†
Comment on the order of these groups in relation to Lagrange's theorem.

[3 marks]

† The proper subgroups exclude the two trivial subgroups which are the subgroup of order 1 that contains only the identity element and the subgroup of order 6 that is a copy of the whole group.

Question 5
Open University Examination Question from October 1992, M101, Q16

Consider the group G with the following Cayley table,

$\times_{10}$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

(i) What is the identity element of G ?
Give a brief reason for your answer.

[2 marks]

(ii) Write down the inverse of 8

[1 mark]

(iii) Find all the cyclic subgroups of G, giving a generator in each case.

[3 marks]

(iv) Is G a cyclic group ?
Give a brief reason for your answer.

[2 marks]

Question 6

The set $S = \{1, 3, 7, 9, 11, 13, 17, 19\}$ forms a group under multiplication modulo 20

(i) Explain why S cannot have a subgroup of order 3

[1 mark]

(ii) Find the order of each element of S

[3 marks]

(iii) Find three different subgroups of S, each of order 4

[4 marks]

4.7 Answers

4.7.1 Solution to 4.2 Example (Teaching Video)

For the group D_4 find $\langle r^3 \rangle$, the subgroup generated by the element r^3

$*$	e	r	r^2	r^3	y	x	p	n
e	e	r	r^2	r^3	y	x	p	n
r	r	r^2	r^3	e	n	p	y	x
r^2	r^2	r^3	e	r	x	y	n	p
r^3	r^3	e	r	r^2	p	n	x	y
y	y	p	x	n	e	r^2	r^3	r
x	x	n	y	p	r^2	e	r	r^3
p	p	x	n	y	r	r^3	e	r^2
n	n	y	p	x	r^3	r	r^2	e

$$\begin{aligned}(r^3)^2 &= r^3 \circ r^3 \\ &= r^2 \qquad \text{from the Cayley table}\end{aligned}$$

$$\begin{aligned}(r^3)^3 &= r^3 \circ (r^3 \circ r^3) \\ &= r^3 \circ r^2 \\ &= r \qquad \text{from the Cayley table}\end{aligned}$$

$$\begin{aligned}(r^3)^4 &= (r^3 \circ r^3) \circ (r^3 \circ r^3) \\ &= r^2 \circ r^2 \\ &= e \qquad \text{from the Cayley table}\end{aligned}$$

In addition to r^2, r and e, for closure there is $r^3 \circ e = r^3$

The subgroup generated by r^3, $\langle r^3 \rangle$, is thus $H = \{ e, r, r^2, r^3 \}$

$|H| = 4$ The subgroup H has order 4

$|r^3| = 4$ The element r^3 has order 4

[3 marks]

4.7.2 Solutions to 4.6 Exercise

Answer 1

(i) The shape does not have any lines of mirror symmetry.

[1 mark]

(ii) The shape does have rotational symmetry, it is of order 4

[1 mark]

(iii) The symmetry group will be cyclic.

[1 mark]

(iv) a corresponds to is a rotation of 180°

[1 mark]

(v) $|a| = 2$, because $a^2 = e$ where e is the identity element.

[1 mark]

(vi) With e as identity element, and $*$ being composition of symmetries,

$*$	e	a
e	e	a
a	a	e

[2 marks]

Answer 2

(i)

Element	Subgroup Generated	Element's Order
0	$\langle 0\rangle = \{0\}$	1
1	$\langle 1\rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$	12
2	$\langle 2\rangle = \{0, 2, 4, 6, 8, 10\}$	6
3	$\langle 3\rangle = \{0, 3, 6, 9\}$	4
4	$\langle 4\rangle = \{0, 4, 8\}$	3
5	$\langle 5\rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$	12
6	$\langle 6\rangle = \{0, 6\}$	2
7	$\langle 7\rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$	12
8	$\langle 8\rangle = \{0, 4, 8\}$	3
9	$\langle 9\rangle = \{0, 3, 6, 9\}$	4
10	$\langle 10\rangle = \{0, 2, 4, 6, 8, 10\}$	6
11	$\langle 11\rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$	12

[6 marks]

(ii) It's cyclic as the whole group can be generated from one element.

[2 marks]

Answer 3

(i) The group is of order 8

[1 mark]

(ii) $\langle a \rangle = \{e, a, a^2, a^3\} \quad \therefore |a| = 4$

$\langle b \rangle = \{e, b, a^2, b\,a^2\} \quad \therefore |b| = 4$

[2 marks]

(iii) $b * ba = a^3$

[1 mark]

(iv) $\left(ba^2 \right)^{-1} = b$

[1 mark]

(v) The cyclic order 4 subgroup is $\langle a \rangle = \langle a^3 \rangle = H = \{e, a, a^2, a^3\}$

Less obviously, $I = \{e, a^2, b, ba^2\}$ or $J = \{e, a^2, ba, ba^3\}$

[1 mark]

(vi) Lagrange's theorem tells us that subgroups of order 3, 5, 6 and 7 can not exist for this group of order 8.

[1 mark]

Answer 4

(i) The identity element is e

[1 mark]

(ii) $\langle a \rangle = \{e, a, c\} \quad \therefore |a| = 3$

$\langle b \rangle = \{e, a, b, c, d, f\} \quad \therefore |b| = 6$

$\langle c \rangle = \{e, a, c\} \quad \therefore |c| = 3$

$\langle d \rangle = \{e, a, b, c, d, f\} \quad \therefore |d| = 6$

$\langle e \rangle = \{e\} \quad \therefore |e| = 1$

$\langle f \rangle = \{e, f\} \quad \therefore |f| = 2$

[3 marks]

(iii) $a^{-1} = c \qquad b^{-1} = d \qquad c^{-1} = a$

$d^{-1} = b \qquad e^{-1} = e \qquad f^{-1} = f$

[3 marks]

(iv) G is cyclic as it can be generated by a single element, b or d

[2 marks]

(v) $\langle f \rangle = \{e, f\}$ of order 2, $\langle a \rangle = \langle c \rangle = \{e, a, c\}$ of order 3

(The subgroups of a cyclic group have to be cyclic)

Lagrange states that the possible subgroups of a group of order 6 must be divisors of 6, that is, 1, 2, 3 or 6, which is consistent with those listed.

[3 marks]

Answer 5

(i) The identity element of G is 6

Various reasons can be given.

For example, it's the only element (in this case) for which $e \times e = e$

[2 marks]

(ii) $8^{-1} = 2$

[1 mark]

(iii) $\langle 2 \rangle = \{2, 4, 6, 8\}$

$\langle 4 \rangle = \{4, 6\}$

$\langle 6 \rangle = \{6\}$

$\langle 8 \rangle = \{2, 4, 6, 8\}$

Thus, G has 3 subgroups, $\{6\}$ generated by 6

$\{4, 6\}$ generated by 4

$\{2, 4, 6, 8\}$ generated by 2 or by 8

[3 marks]

(iv) Yes, G is a cyclic group because it can be generated by a single element, either 2 or 8

[2 marks]

Answer 6

It may help to be shown the Cayley table for the group;

$\times_{20}$	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

(i) The group S is of order 8

Lagrange's theorem states that the order of any subgroup must be a divisor of the order of the group.

The divisors of 8 are 1, 2, 4, 8.

$\therefore$ As 3 is not a divisor of 8, S can not have a subgroup of order 3 ☐

[1 mark]

(ii)

$\langle 1 \rangle = \{1\} \qquad \therefore \ |1| = 1$

$\langle 3 \rangle = \{1,\ 3,\ 7,\ 9\} \qquad \therefore \ |3| = 4$

$\langle 7 \rangle = \{1,\ 3,\ 7,\ 9\} \qquad \therefore \ |7| = 4$

$\langle 9 \rangle = \{1,\ 9\} \qquad \therefore \ |9| = 2$

$\langle 11 \rangle = \{1, 11\} \qquad \therefore \ |11| = 2$

$\langle 13 \rangle = \{1,\ 9,\ 13,\ 17\} \qquad \therefore \ |13| = 4$

$\langle 17 \rangle = \{1,\ 9,\ 13,\ 17\} \qquad \therefore \ |17| = 4$

$\langle 19 \rangle = \{1,\ 19\} \qquad \therefore \ |19| = 2$

[3 marks]

(iii) Two cyclic subgroups of order 4 were found above.

They are $\{1, 3, 7, 9\}$ along with $\{1, 9, 13, 17\}$.

The question wants us to find another subgroup of order 4.

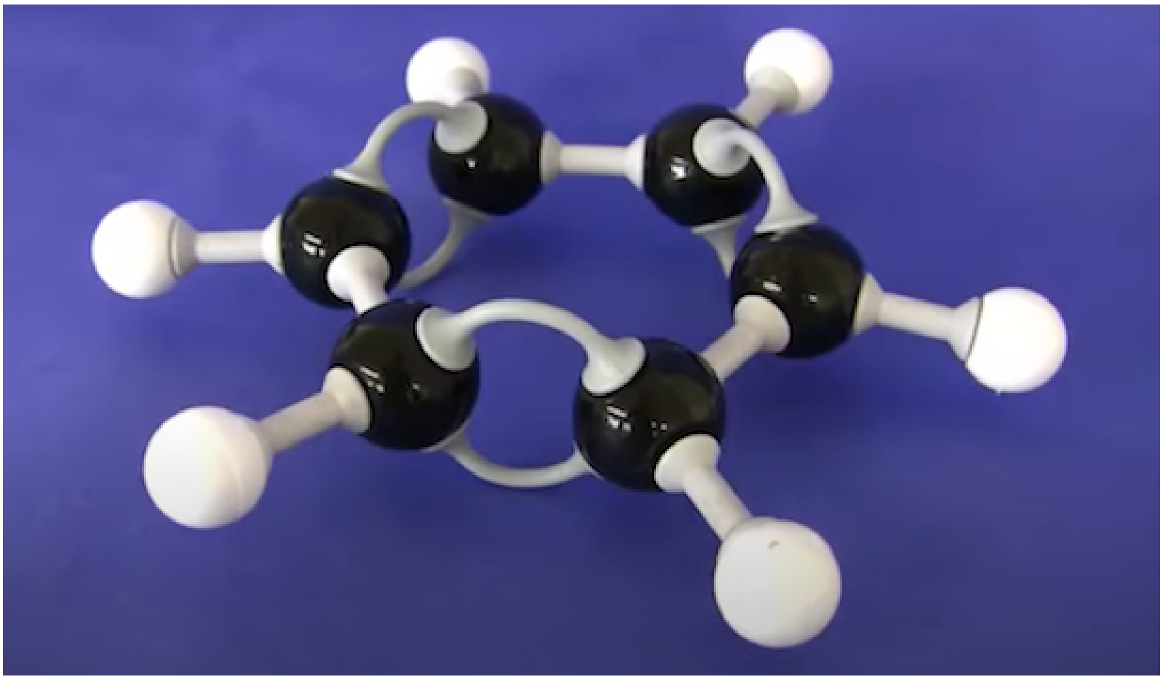
It can't be cyclic, or it would have been detected in the part (ii) answer.

After some playing around I found $\{1, 9, 11, 19\}$

[4 marks]

5.1 Isomorphism

One aim of group theory is to capture the symmetries of various entities, be they, for example, a geometric shape, a set of functions, or a set of numbers under modulo arithmetic. However, its reach is broader than that, Recently, for example, group theory predicted the existence of a tiny particle in physics. Knowing roughly what to look for, this was then detected in the physical world. Another application of group theory is in the study of crystals in Chemistry.



A model of the molecule Benzine

Group theory reveals that there are limits on the types of structure that symmetrical objects can have. For example, when the order of a group is a prime number, there is only one fundamental group of that order and that it has to be cyclic. Seemingly, different groups of that order have the same underlying structure; mathematicians say they are “isomorphic". As a further example, there are only two possible groups of order 6, one cyclic and one not. So any group of order 6 has to be isomorphic to one of those two groups. Thus, what may have initially seems like a bewildering array of groups is actually more constrained. Group theory is the tool that can identify what those constraints are.

5.2 A Catalogue of Possible Groups

On the next page is a catalogue of all possible groups of order less than 12. Faced with an unknown group of order less than 12, the natural question to ask is which group from this catalogue is the unknown group isomorphic to. Spotting an isomorphism using Cayley tables can be tricky; the catalogue lists each group's defining properties. Matching these is often the easier option.

Order	Name	Examples	Properties
1	$\mathbb{Z}_1$	Trivial group	Only group of order 1
2	$\mathbb{Z}_2$	$\{0, 1\}$ under $+_2$	Only group of order 2
3	$\mathbb{Z}_3$	$\{0, 1, 2\}$ under $+_3$	Only group of order 3
4	$\mathbb{Z}_4$	$\{0, 1, 2, 3\}$ under $+_4$	Cyclic group of order 4
	$K_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$	Klein group Symmetry group of a rectangle	Not cyclic. Every element (except identity) has order 2
5	$\mathbb{Z}_5$	$\{0, 1, 2, 3, 4\}$ under $+_5$	Cyclic group of order 5
6	$\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2$	$\{0, 1, 2, 3, 4, 5\}$ under $+_6$	Cyclic group of order 6
	S_3, D_4	All permutations of 3 objects, Equilateral triangle's symmetry	Not cyclic $\therefore$ no element of order 6
7	$\mathbb{Z}_7$	$\{0, 1, 2, 3, 4, 5, 6\}$ under $+_7$	Cyclic group of order 7
8	$\mathbb{Z}_8$	$\{0, 1, 2, 3, 4, 5, 6, 7\}$ under $+_8$	Cyclic group of order 8
	D_4	Symmetry group of a square (Some text books call this D_8)	Not cyclic $\therefore$ no element of order 8 Exactly 2 elements of order 4
	$\mathbb{Z}_4 \times \mathbb{Z}_2$	Rational points on the elliptic curve $y^2 = (x + 3)x(x - 1)$	Not cyclic $\therefore$ no element of order 8 Exactly 4 elements of order 4
	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	Symmetry group of a cuboid	Not cyclic $\therefore$ no element of order 8 Every element (except identity) has order 2
	Q_4	Quaternion group	Not cyclic $\therefore$ no element of order 8 Exactly 6 elements of order 4
9	$\mathbb{Z}_9$	$\{0, 1, 2, 3, 4, ..., 8\}$ under $+_9$	Cyclic group of order 9
	$\mathbb{Z}_3 \times \mathbb{Z}_3$		Not cyclic $\therefore$ no element of order 9 Exactly 4 elements of order 3
10	$\mathbb{Z}_{10} = \mathbb{Z}_5 \times \mathbb{Z}_2$	$\{0, 1, 2, 3, 4, ..., 9\}$ under $+_{10}$	Cyclic group of order 10
	D_5	Frobenius group (Some text books call this D_{10})	Not cyclic $\therefore$ no element of order 10
11	$\mathbb{Z}_{11}$	$\{0, 1, 2, 3, 4, ..., 10\}$ under $+_{11}$	Cyclic group of order 11

5.3 Example

The Cayley tables for two groups of order 6 are presented below.
The first is for multiplication modulo 7 on the set {1, 2, 3, 4, 5, 6}
The second is for addition modulo 6 on the set {0, 1, 2, 3, 4, 5}
Are these two groups isomorphic or not ?

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Teaching Video: http://www.NumberWonder.co.uk/v9108/5.mp4

The video talks through to solution presented on the next page

[6 marks]

5.4 Where Do Mathematicians' Go When They Die ?

The Symmetry

5.5 Solution to the 5.3 Example

Start by identifying each group's identity element which is easy from a Cayley table; simply look for the row that matches the column headings.
Circle all locations of the identity in both tables.

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

At this stage it's not clear if the two are isomorphic or not.
If an isomorphism, *f*, exists it must map one identity onto the other.

$$f(1) = 0$$

From the catalogue of groups it is known that there are two groups of order 6. One is cyclic and one is not.
The catalogue also states that the set {0, 1, 2, 3, 4, 5} under $+_6$ is cyclic.
(That is, under addition, modulo 6)
So if it can be shown that the multiplication modulo 7 group is also cyclic then the two must be isomorphic. On the other hand, if the multiplication modulo 7 group is not cyclic, then no isomorphism between the two exists.

If the modulo 7 group is cyclic it will be possible to generate the entire group from at least one of it's elements.
Starting to work through {1, 2, 3, 4, 5, 6 } using each element as a generator;

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{1, 2, 4\}$

$\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\}$ $\therefore$ The modulo 7 group is cyclic

$\therefore$ The two groups are isomorphic.

The question does not ask for any more details but, out of interest, here is the isomorphism made plain by manipulating one of the Cayley tables;

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$+_6$	0	2	1	4	5	3
0	0	2	1	4	5	3
2	2	4	3	0	1	5
1	1	3	2	5	0	4
4	4	0	5	2	3	1
5	5	1	0	3	4	2
3	3	5	4	1	2	0

5.6 Describing an Isomorphism Mathematically

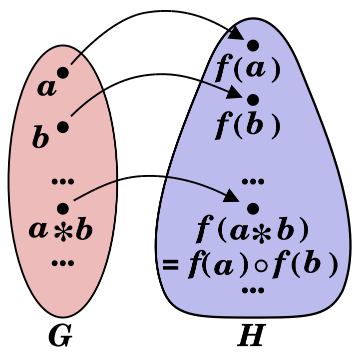
Intuitively, isomorphic groups have the same symmetry, structured in the same way. Given that an isomorphism exists between two groups G and H, all of the key properties of G are to be found in H such as, for example, the number and order of the various subgroups and the number and order of the various elements. In particular, if G is cyclic then so too is H.

Formally, an isomorphism is described as follows;

Definition : Isomorphism

Two groups $(G, *)$ and $(H, \circ)$ are isomorphic, written $G \cong H$, if there exists a mapping f that maps G onto H in the following manner;

- f maps all of the elements of G onto all of the elements of H
- f maps each element of G to a different element of H
- f preserves the structure $f(a * b) = f(a) \circ f(b)$

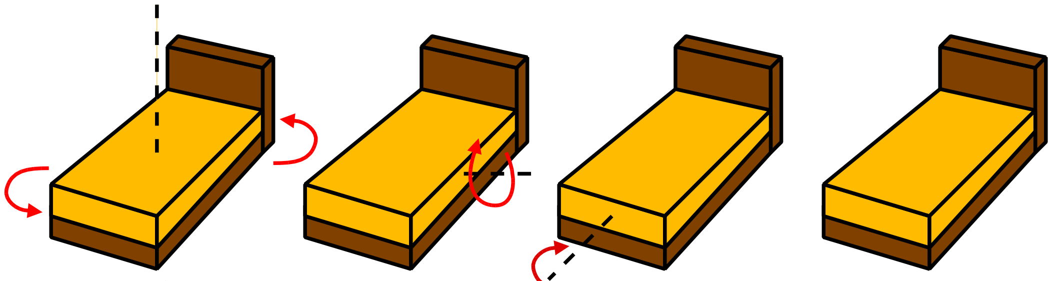


5.7 Exercise

Marks Available: 40

Question 1

A mattress manufacturer suggests that customers "flip" their mattress regularly so that it wears out evenly. The following instructions are provided:



The operation ∘ is defined on $\{A, B, C, D\}$ as "followed by" so that, for example, $A \circ C$ means "flip about the long axis followed by rotate 180°"

(i) Complete the Cayley table for these four options;

∘	***A***	***B***	***C***	***D***
A				
B		***D***		
C	***B***			
D				***D***

[3 marks]

(ii) Which element is the identity element ?

[1 mark]

There are two groups of order 4.

One is the cyclic group $\mathbb{Z}_4$, the other is the (non-cyclic) Klein group, K_4

(iii) Work out the order of each of the elements A, B, C and D.

[2 marks]

(iv) Is the group of mattress transformations cyclic ?

[1 mark]

(v) State if the mattress transformations group is isomorphic to $\mathbb{Z}_4$ or K_4

[1 mark]

Question 2

The Catalogue of Possible Groups list five fundamental groups of order 8.

They are $\mathbb{Z}_8$, D_4, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and Q_4

Shown below is the Cayley table for an unknown group of order 8.

$*$	s	a	k	m	w	z	c	p
s	m	z	w	s	k	a	p	c
a	z	m	p	a	c	s	w	k
k	w	p	m	k	s	c	z	a
m	s	a	k	m	w	z	c	p
w	k	c	s	w	m	p	a	z
z	a	s	c	z	p	m	k	w
c	p	w	z	c	a	k	m	s
p	c	k	a	p	z	w	s	m

(i) Which element is the identity element ?

[1 mark]

(ii) List the inverse of each element.

[2 marks]

(iii) Is the Cayley table of a cyclic group ?
Give a reason for your answer.

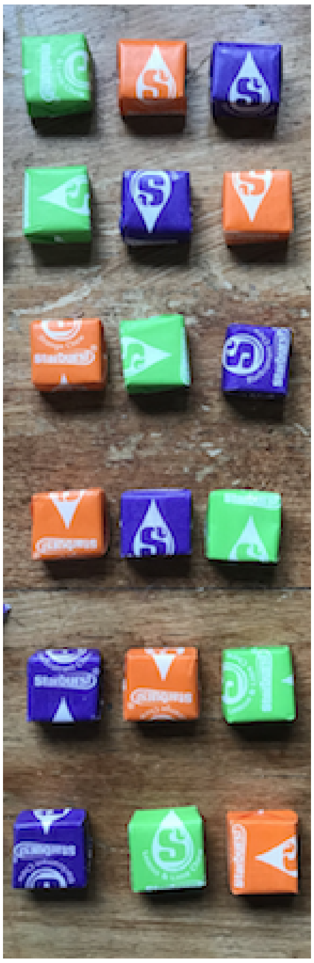
[2 marks]

(iv) To which of the possible fundamental groups of order 8 is the unknown group isomorphic ?
Give a reason for your answer.

[2 marks]

Question 3

Michael has a bag of Starburst™ sweets and has worked out that there are six different ways of arranging one each of the colours Green, Orange, and Purple.



$$e = \begin{pmatrix} G & O & P \\ G & O & P \end{pmatrix}$$

$$r = \begin{pmatrix} G & O & P \\ G & P & O \end{pmatrix}$$

$$s = \begin{pmatrix} G & O & P \\ O & G & P \end{pmatrix}$$

$$t = \begin{pmatrix} G & O & P \\ O & P & G \end{pmatrix}$$

$$u = \begin{pmatrix} G & O & P \\ P & O & G \end{pmatrix}$$

$$v = \begin{pmatrix} G & O & P \\ P & G & O \end{pmatrix}$$

Michael suspects that the set $\{e, r, s, t, u, v\}$ under the binary operation "followed by" forms a group $(G, *)$ where, for example, $s * t$ means t followed by s.

(i) Show that $s * t = r$ by using two-row notation

[2 marks]

(ii) Show that $s * t \neq t * s$

[2 marks]

(iii) What is the inverse of the element s ?
Is it e, r, s, t, u or v ?
Give a reason for your answer.

[2 marks }

(iv) Construct the Cayley table for the proposed group $(G, *)$

$*$	e	r	s	t	u	v
e	e	r	s			
r	r	e				
s	s					
t						e
u					e	r
v				e	s	t

[4 marks]

(v) Show that $(G, *)$ is a group. You may assume associativity.

[3 marks]

(vi) Which of the groups of order 6, $\mathbb{Z}_6$ or S_3, is G isomorphic to ?
Give a reason for your answer.

[2 marks]

Question 4

The set $G = \{1, 7, 11, 13, 17, 19, 23, 29\}$ forms a group under multiplication modulo 30.

(i) Find the order of each element of this group.

[4 marks]

(ii) Find a cyclic subgroup of G of order 4

[2 marks]

(iii) Find a subgroup of G which is isomorphic to the Klein four-group.

[2 marks]

The set $H = \{0, 1, 2, 3, 4, 5, 6, 7\}$ forms a group under addition modulo 8.

(iv) State, with reasons, whether $G \cong H$

[2 marks]

5.8 Answers to 5.7 Exercise

Answer 1

(i)

$\circ$	A	B	C	D
A	D	C	B	A
B	C	D	A	B
C	B	A	D	C
D	A	B	C	D

[3 marks]

(ii) D is the identity element.

[1 mark]

(iii) $A^2 = B^2 = C^2 = D$ (the identity element)

So A, B and C are of order 2, with D having order 1

[2 marks]

(iv) The group of mattress transformations is not cyclic because none of the elements was of order 4.

That is, none of the elements will generate the whole group.

[1 mark]

(v) The mattress transformations group is isomorphic to K_4 as that is the only fundamental group of order 4 that is not cyclic.

[1 mark]

Answer 2

(i) m is the identity element

Look for the yellow row that is the same as the red row and the green element at the start of that yellow row is the identity element.

[1 mark]

(ii) Every element is its own inverse !

The quick way to spot this from the diagonal on the Cayley table.

Every element on that diagonal is, m the identity element.

Here is a short proof that s is its own inverse;

$$
\begin{aligned}
s * s &= m \\
s^{-1} * (s * s) &= s^{-1} * m && \text{Pre multiply both sides by } s^{-1} \\
(s^{-1} * s) * s &= s^{-1} && \text{Associativity} \\
m * s &= s^{-1} \\
s &= s^{-1}
\end{aligned}
$$

[2 marks]

(iii) The table is not of a Cyclic group because all of the elements are of order 2 except the identity which is of order 1.

No element is of order 8. That is, no element generates the whole group.

$\therefore$ The group is not cyclic.

[2 marks]

(iv) From the Catalogue of known groups, the only group that has order 8 and all elements of order 2 is the group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and so the unknown group must be isomorphic to this.

[2 marks]

Answer 3

(i)

$$\begin{aligned} \text{LHS} &= s * t \\ &= \begin{pmatrix} G & O & P \\ O & G & P \end{pmatrix} * \begin{pmatrix} G & O & P \\ O & P & G \end{pmatrix} \\ &= \begin{pmatrix} G & O & P \\ G & P & O \end{pmatrix} \\ &= r \\ &= \text{RHS} \qquad \square \end{aligned}$$

[2 marks]

(ii)

$$\begin{aligned} t * s &= \begin{pmatrix} G & O & P \\ O & P & G \end{pmatrix} * \begin{pmatrix} G & O & P \\ O & G & P \end{pmatrix} \\ &= \begin{pmatrix} G & O & P \\ P & O & G \end{pmatrix} \\ &= u \\ &\neq s * t \qquad \square \end{aligned}$$

[2 marks]

(iii)

$$\begin{aligned} s^{-1} &= \begin{pmatrix} G & O & P \\ O & G & P \end{pmatrix}^{-1} \\ &= \begin{pmatrix} G & O & P \\ O & G & P \end{pmatrix} \\ &= s \qquad \text{It's self inverse} \end{aligned}$$

[2 marks]

(iv)

$*$	e	r	s	t	u	v
e	e	r	s	t	u	v
r	r	e	v	u	t	s
s	s	t	e	r	v	u
t	t	s	u	v	r	e
u	u	v	t	s	e	r
v	v	u	r	e	s	t

[4 marks]

(v) Closure : From the Cayley table it is observed that all possible combinations of two elements from the set $\{e, r, s, t, u, v\}$ yield only elements already in that set.

$\therefore\ (G, *)$ is closed

Identity : The set has a unique identity, e

Inverses : The inverse of e is e
The inverse of r is r
The inverse of s is s
The inverse of t is v
The inverse of u is u
The inverse of v is t

$\therefore$ Each element of G has a unique inverse

With the assumption that associativity holds, the axioms for G to be a group have been shown to be satisfied.

[3 marks]

(vi) This question has looked at the set of permutations of three objects which The Catalogue of all Possible Groups calls S_3
Other answers are possible such as showing the group is not cyclic.

[2 marks]

Answer 4

$\times_{30}$	1	7	11	13	17	19	23	29
1	1	7	11	13	17	19	23	29
7	7	19	17	1	29	13	11	23
11	11	17	1	23	7	29	13	19
13	13	1	23	19	11	7	29	17
17	17	29	7	11	19	23	1	13
19	19	13	29	7	23	1	17	11
23	23	11	13	29	1	17	19	7
29	29	23	19	17	13	11	7	1

(i) $\langle 1 \rangle = \{1\}$ $\quad |1| = 1$

$\langle 7 \rangle = \{1, 7, 13, 19\}$ $\quad |7| = 4$

$\langle 11 \rangle = \{1, 11\}$ $\quad |11| = 2$

$\langle 13 \rangle = \{1, 7, 13, 19\}$ $\quad |13| = 4$

$\langle 17 \rangle = \{1, 17, 19, 23\}$ $\quad |17| = 4$

$\langle 19 \rangle = \{1, 19\}$ $\quad |19| = 2$

$\langle 23 \rangle = \{1, 17, 19, 23\}$ $\quad |23| = 4$

$\langle 29 \rangle = \{1, 29\}$ $\quad |29| = 2$

[4 marks]

(ii) The part (i) answer found two cyclic subgroups of order 4.
They are, {1, 7, 13, 19} or {1, 17, 19, 23}

[2 marks]

(iii) The Klein four-group, K_4 is not cyclic.
One idea is to start with a cyclic subgroup of order 2, and add an
from one of the other subgroups of order 2 that's not is a cyclic subgroup.
$\{1, 11, \_\_, 29\} \Rightarrow \{1, 11, 19, 29\}$ which is isomorphic to K_4

[2 marks]

(iv) H is isomorphic to $\mathbb{Z}_8$ which is cyclic (from the Catalogue)
$\therefore$ As G in not cyclic it is not isomorphic to H

[2 marks]

6.1 Revision

Here is the formal definition of a group;

The Definition of a Group

If G is a set and $*$ is a binary operation defined on G, then $(G, *)$ is a group if the following four axioms hold:

- **Closure:** For all $a, b \in G$, $a * b \in G$
- **Identity:** There exists an identity element $e \in G$.
  This is such that, for all $a \in G$, $a * e = e * a = a$
- **Inverses:** For each $a \in G$, there exists an inverse element $a^{-1} \in G$
  This is such that $a * a^{-1} = a^{-1} * a = e$
- **Associativity:** For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$

And a reminder of Lagrange's theorem;

Lagrange's Theorem

If H is a subgroup of a finite group G, the order of H divides the order of G.

6.2 Exercise

Marks Available: 40

Question 1

Solve the following congruence equation modulo 8.
Any answers should be given as elements from the set of least residues modulo 8.

$$2x - 9 \equiv 5 \pmod 8$$

[3 marks]

Question 2
Consider the following binary operation table;

$\circ$	a	b	c	d
a	c	d	c	b
b	d	c	b	a
c	a	d	c	d
d	b	a	b	c

(a) Explain why the set of elements $\{a, b, c, d\}$ do **not** form a group.

[1 mark]

(b) Given the binary operation table, calculate

(i) $c \circ d$

[1 mark]

(ii) $a \circ (c \circ b)$

[1 mark]

(iii) $(a \circ c) \circ b$

[1 mark]

(iv) $(d \circ c) \circ (b \circ a)$

[1 mark]

(c) **(i)** Does the expression $a \circ b \circ c$ make sense ?
State your answer as either “Yes” or “No”

[1 mark]

(ii) Give a reason for your (c)(i) answer.

[1 mark]

Question 3

The set $G = \{ 1, 3, 5, 9, 11, 13 \}$ forms a group under multiplication modulo 14.

(i) Complete the following Cayley table for this group;

$\times_{14}$	**1**	**3**	**5**	**9**	**11**	**13**
1			**5**			
3		**9**				
5						
9				**11**		
11		**5**				
13						**1**

[2 marks]

(ii) Explain why $(G, *)$ can have no subgroup of order 4

[2 marks]

(iii) Find a subgroup of order 2 and construct its Cayley table.

$\times_{14}$		

[1 mark]

(iv) Find a subgroup of order 3 and construct its Cayley table.

$\times_{14}$			

[2 marks]

Question 4

Further A-Level, Pure Mathematics 2, June 2022, Paper 4A, Q1 (Edexcel)

The group S_4 is the set of all possible permutations that can be performed on the four numbers 1, 2, 3 and 4, under the operation of composition.

For the group S_4

(a) write down the identity element,

[1 mark]

(b) write down the inverse of the element a, where

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

[1 mark]

(c) demonstrate that the operation of composition is associative using the following elements

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \qquad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \qquad \text{and} \qquad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

[2 marks]

(d) Explain why it is possible for the group S_4 to have a subgroup of order 4. You do not need to find such a subgroup.

[2 marks]

Question 5

Further A-Level, Pure Mathematics 2, June 2024, Paper 4A, Q7 (Edexcel)

The set of matrices $G = \{\mathbf{I}, \mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}\}$ where

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \mathbf{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\mathbf{C} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \mathbf{D} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \mathbf{E} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

with the operation $\otimes_2$ of matrix multiplication with entries evaluated modulo 2, forms a group.

(a) Show that **B** is an element of order 3 in G

[2 marks]

(b) Determine the orders of the other elements of G

[3 marks]

(c) Give a reason why G is **not** isomorphic to

(i) a cyclic group of order 6

(ii) the group of symmetries of a regular hexagon

[2 marks]

The group H of permutations of the numbers 1, 2 and 3 contains the following elements, denoted in two-line notation,

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad d = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

(d) Determine an isomorphism between the groups G and H

[3 marks]

Question 6

Given $\mathbb{Z}_2 = \{0,1\}$, the Cartesian product

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$$

has *four* elements.

This set inherits a binary structure via addition of co-ordinates

$$(x, y) + (v, w) := (x + v, y + w)$$

where $x + v$ and $y + w$ are both computed in $(\mathbb{Z}_2, +_2)$.

This binary operation has an addition table that should look very familiar: it has exactly the same structure as the Klein four-group!

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

$\cong$

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

We conclude that $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong K_4$ is indeed a group

(a) List the elements of the Cartesian product of $(\mathbb{Z}_3, +_3)$ and $(\mathbb{Z}_2, +_2)$

[3 marks]

(b) Determine $\langle(1,1)\rangle$

[2 marks]

(c) Use your answers to parts (a) and (b) to deduce which group $\mathbb{Z}_3 \times \mathbb{Z}_2$ is isomorphic to.

[2 marks]

6.3 Answers

Answer 1

$$2x - 9 \equiv 5 \pmod 8$$
$$2x \equiv 14 \pmod 8$$
$$2x \equiv 14,\ 22,\ 30,\ \ldots \pmod 8$$
$$x \equiv 7,\ 3 \pmod 8$$

This could be more succinctly written as $x \equiv 3 \pmod 4$

[3 marks]

Answer 2

$\circ$	a	b	c	d
a	c	d	c	b
b	d	c	b	a
c	a	d	c	d
d	b	a	b	c

(a) A necessary condition for the set to form a group in that its elements form a Latin Square in the binary operation table. In other words each element occurs once and once only in each row and in each column. This is not so in this case. For example, c occurs twice in the top row.

[1 mark]

(b) **(i)** $c \circ d = d$

[1 mark]

(ii) $a \circ (c \circ b) = a \circ d = b$

[1 mark]

(iii) $(a \circ c) \circ b = c \circ b = b$

[1 mark]

(iv) $(d \circ c) \circ (b \circ a) = b \circ d = a$

[1 mark]

(c) **(i)** No

[1 mark]

(ii) How the expression is bracketed makes a difference to the answer. In other words, associativity does not hold.
On the one hand, $a \circ (b \circ c) = a \circ b = d$
but on the other, $(a \circ b) \circ c = d \circ c = b$
To make sense brackets need to be present to show which of the two possible interpretations is wanted.

[1 mark]

Answer 3

(i)

$\times_{14}$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

[3 marks]

(ii) The given group, $(G, \times_{14})$, has order 6.

By Lagrange's theorem, the order of a subgroup of must divide the order of the group of which it is a subgroup.

$\therefore$ $(G, \times_{14})$ can only have subgroups of order 1, 2, 3 or 6

$\therefore$ $(G, \times_{14})$ has no subgroup of order 4 $\square$

[2 marks]

(iii) $H = \{ 1, 13 \}$

$\times_{14}$	1	13
1	1	13
13	13	1

[1 mark]

(iv)

$\times_{14}$	1	9	11
1	1	9	11
9	9	11	1
11	11	1	9

[3 marks]

Answer 4

(a) The identity element is the “do nothing” permutation;

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

[1 mark]

(b) To undo the given permutation;

$$a^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

[1 mark]

(c) We need to demonstrate that $a \circ \{ b \circ c \} = \{ a \circ b \} \circ c$

$$\begin{aligned} \text{RHS} &= a \circ \{ b \circ c \} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \right\} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \right\} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \text{LHS} &= \left\{ \begin{matrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{matrix} \right) \circ \left. \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \right\} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \\ &= \left\{ \left\{ \begin{matrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{matrix} \right\} \right\} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \\ &= \text{RHS} \qquad \square \end{aligned}$$

[2 marks]

(d) S_4 is of order 24. (From 4! = 24)

Possible subgroups, by Lagrange's Theorem, will be factors of 24.

As 4 is a factor of 24, it is possible that there is a subgroup of order 4.

[2 marks]

Answer 5

(a) Looking for the power of **B** that gives the identity matrix **I**;

$$\mathbf{B} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \mathbf{I}$$

$$\mathbf{B}^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \neq \mathbf{I} \qquad \text{(mod 2)}$$

$$\mathbf{B}^3 = \mathbf{B}^2\mathbf{B} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I} \qquad \text{(mod 2)}$$

Thus, $|\mathbf{B}| = 3$, as expected.

[2 marks]

(b) $|\mathbf{I}| = 1$, $|\mathbf{A}| = 2$, $|\mathbf{C}| = 2$, $|\mathbf{D}| = 2$, $|\mathbf{E}| = 3$

[3 marks]

(c) **(i)** To be a cyclic group there must be at least one element that generates the whole group.
No element generated the whole group.
In other words, no element was of order 6 (From part (b))
So G is not isomorphic to a cyclic group of order 6.

(ii) A regular hexagon has 12 symmetries.
(6 rotational and 6 lines of mirror symmetry)
So the group of these symmetries will be of order 12.
Our group, G, is of order 6.
A necessary condition for two groups to be isomorphic is that they are of the same order. So G is not isomorphic to the group of symmetries of a regular hexagon.

[2 marks]

(d) The six possible matchings of elements are given in the following table (only one is required)

I	**A**	**B**	**C**	**D**	**E**
e	c	a	d	f	b
e	d	a	f	c	b
e	f	a	c	d	b
e	c	b	f	d	a
e	d	b	c	f	a
e	f	b	d	c	a

[3 marks]

Answer 6

(a) $\mathbb{Z}_3 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)\}$

[3 marks]

(b) $\langle(1,1)\rangle = \{(1,1), (2,0), (0,1), (1,0), (2,1), (0,0)\}$

(Listed in the order they are generated)

[2 marks]

(c) As $\langle(1,1)\rangle$ has generated the whole group, $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$ the cyclic group of order 6.

[2 marks]